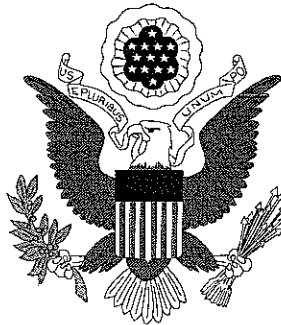


Misc. 06-170 (SAF)

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO**



RECEIVED AND FILED
2006 AUG -8 PM 12:44
CLERK'S OFFICE
U.S. DISTRICT COURT
SAN JUAN, P.R.

**POLICY REGARDING LIMITED PERSONAL USE OF
GOVERNMENT EQUIPMENT,
INCLUDING INFORMATION TECHNOLOGY
(Revised May 4, 2006)**

POLICY REGARDING LIMITED PERSONAL USE OF GOVERNMENT EQUIPMENT, INCLUDING INFORMATION TECHNOLOGY

I. AUTHORITY

Generally, chambers personnel and Court Unit employees may use Government office equipment for authorized purposes only. As set forth below, limited personal use of government office equipment by chambers personnel and Court Unit employees during non-work time is considered to be an "authorized use" of government property. Authority for this policy is derived from a resolution by the Judicial Conference of the United States.

Authority to use government equipment and to access sites on the Internet and J-Net through a Web browser is vested in the Judicial Officers and Court Unit Executives, for members of their respective staffs. Authority to configure a Court-owned personal computer to gain access to these resources is vested exclusively with the Clerk of Court, through the Systems Department.

II. GENERAL POLICY

Chambers personnel and Court Unit employees are permitted limited use of government equipment for personal needs if the use does not interfere with official business and involves minimal additional expenses to the Government. This limited personal use of government office equipment should take place during the employee's non-work time. This privilege to use government office equipment for non-government purposes may be revoked or limited at any time.

A. Definitions

For the purposes of this policy:

Court Unit means the Clerk's Office, the U.S. Pretrial Services Office, and the U.S. Probation Office within the U.S. District Court for the District of Puerto Rico.

Judicial Officer means an active judge, senior judge, and magistrate judge.

Court Unit Executive means the Clerk of Court, the Chief U.S. Pretrial Services Officer, and the Chief U.S. Probation Officer.

Employee means chambers personnel and Court Unit employees (including interns, students and contractors).

Systems Department means the Information Technology (IT) section at the U.S. District Court Clerk's Office, which supplies and supports all the IT functions for the U.S. District Court, U.S. Pretrial Services, and the U.S. Probation Office.

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 2

Privilege means that the Court is extending the opportunity to its employees to use government property for limited personal use in an effort to create a more supportive work environment. However, this policy does not create a right to use government office equipment for non-government purposes. Moreover, the privilege does not entail the modification of equipment, including loading unauthorized software and/or hardware or performing configuration changes. Such configurations shall only be performed by the Systems Department staff.

Government office equipment includes, but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and e-mail. This list is provided to show examples of office equipment intended to be covered by this policy, and it is not meant to be comprehensive.

Minimal additional expense means that the employee's personal use of government office equipment is limited to those situations where the Government is already providing equipment or services and the use of same will only result in normal wear and tear or the use of small amounts of electricity, ink, toner, paper or other consumable supplies. Examples of minimal additional expenses include, but is not limited to, making few photocopies, using a computer printer to print few pages, making occasional brief phone calls, infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons.

Non-work time means times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use government office equipment during their own off-duty hours such as before or after a workday (subject to chambers and the Court Unit's office hours), lunch periods, authorized breaks, or weekends and holidays (if their duty stations is normally available at such times).

Personal use means activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Government employees are specifically prohibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection for freelancing and self employment. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist anyone in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 3

Savings Plan or other personal bank account, or to seek employment, or communicate with a volunteer organization, or to check the news or weather information.

Information technology means any equipment, software code or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, processing, management, movement control, display, switching, interchange, transmission, or reception of data or information.

B. Inappropriate Personal Uses of Government Equipment

All employees are expected to use good judgment, common sense, and sensibility in the use of government office equipment and thus, refrain from using said equipment for inappropriate activities. Misuse, abuse, inappropriate or prohibited personal use of government office equipment, including information technology, includes; but is not limited to:

1. Any personal use of government office equipment during employees' working hours other than occasional, brief periods.
2. Any personal use that results in loss or decrease of productivity or interference with official duties.
3. Any use that could generate more than minimal additional expense to the Court in areas such as:
 - a. Communications infrastructure costs; e.g., telephone charges, telecommunications traffic, etc.;
 - b. Use of consumables in limited amounts: e.g., paper, ink, toner, etc.;
 - c. Normal wear and tear on equipment;
 - d. Data storage on storage devices;
 - e. Connectivity impacts: e.g., E-mail messages with large attachments, streaming audio or video and downloading large files.

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 4

4. Employees are specifically prohibited from using government office equipment to maintain or support "for profit" activities, other outside employment or a personal private business activity.

Examples of this prohibition include using government office equipment for sale of goods, freelancing, consulting for pay or using a computer and internet connection to run any kind of for-profit personal activity.

- 4.5 Engaging in extended long distance calls for non-official matters.
5. Any personal use that can cause congestion, delay, or disruption of service to any government system or equipment. For example, animated greeting cards, video, sound or other large file attachments degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams (such as radio/TV stations, personal video conferencing or other broadcast services) also degrade the performance of the entire network and are inappropriate use.
6. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
7. Creating, copying, sending or forwarding chain letters or other unauthorized mass mailings regardless of the subject matter.
8. To intentionally participate in activities that promote computer crime or misuse including, but not limited to, posting or disclosing passwords, credit card and other account numbers and system vulnerabilities.
9. Using the government office equipment for activities that are illegal, inappropriate, or offensive to the Court, or to other employees or the public.

Such activities include, but are not limited to: the promulgation or dissemination of hate speech, material that ridicules others on the basis of race, creed, political beliefs, religion, color, gender, disability, national origin, ethnic group or sexual orientation, that harasses or threatens other users with violence or physical harm, libelous or that involves defamation of character.

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 5

10. Creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials.
11. Violating or infringing on the rights of any person, including the right to privacy.
12. The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorists activities, and any other illegal activities or activities otherwise prohibited, etc.
13. Engaging in any outside fund-raising activity, endorsing any product, service or religion, or participating in any lobbying activity or prohibited partisan political activity.
14. Posting Judiciary information to external news groups, bulletin boards or other public or private forums without authority. This includes unauthorized statements regarding Court policies or practices or any use that could create the perception that the communication was made in an official capacity as a judiciary employee, unless appropriate approval has been obtained for uses that may appear to be at odds with the Court's mission or positions.
- 14.5 Electronic transmission of sensitive or confidential information is forbidden.
15. Making unauthorized commitments or promises that might be perceived as binding upon the Court.
16. Engaging in personal discussions through non-work-related chat software, peer-to-peer file sharing, chat rooms, instant messaging, on-line conferences, or other similar forum for communicating with persons or entities outside the judiciary's private data communications network. **(This practice was prohibited by the Judicial Conference of the United States, September 2005 Session).** (See Appendix I).
17. Acquiring, using, transmitting or distributing of any controlled information including computer software and data, that includes privacy, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 6

18. Engaging in extended or recurrent electronic shopping through catalog, auction, or clearing websites.
19. **Accessing personal Internet email accounts from within the judiciary's network is strongly discouraged.** Those having an impending need to access a personal Internet email account from within the Court's network must comply with the following guidelines:
 - a. Do not open any email attachments unless you are absolutely sure they are safe.
 - b. Do not open or follow any links in an email unless you are absolutely sure they are safe.
 - c. Use an Internet email provider which provides virus scanning of email and attachments, such as AOL's AIM Mail, Google Gmail, MSN Hotmail, Yahoo Mail or your local Internet Service provider web-mail page.
 - d. Avoid advertising your personal email name over the Internet.
 - e. Avoid the use of automatic email forwarding to personal Internet email accounts.
20. Any other use prohibited pursuant to the Clerk's Office Employee Personnel Manual and/or any applicable personnel manual to the relevant Court Unit and the Code of Conduct for Judiciary Employees.
21. **Providing the Court's email address or account for commercial email messaging is prohibited.** However, sending and receiving a very limited amount of email in your Lotus Notes court account to address infrequent and sporadic family and personal issues is consistent with this policy.
22. **Downloading and/or installing third party email software to send and/or retrieve personal email through the Court's network is prohibited.**

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 7

C. Specific Provisions on Use of Information Technology

Use of Information Technology is specifically authorized for the following purposes:

1. Research in connection with work assignments;
2. Reading professional literature, or communicating with others to pursue professional and career development, including professional organizations;
3. Expedite administrative duties in direct support of work-related functions;
4. E-mail relating directly to official duties;
5. Limited personal use during employee's non-work time, as stated in this policy.

Downloading large files during business hours can compromise the performance of the entire system. A file which exceeds two (2) megabytes in size should not be attached to an e-mail message sent during normal business hours. Rather, it should be sent outside of normal business hours or be transmitted through alternative means.

Prior to working with large files, employees should consider the impact on all other network users and remember that, files downloaded from the DCN/J-Net or Internet may be infected with a computer virus. It is imperative that all downloaded files be scanned for viruses (both before and after any decompression or decryption) with special software designed for that purpose which has been pre-installed on the user's computer system. In case of doubts about how to use the virus detection software, employees should contact the Systems Department.

Employees are obligated to prevent unauthorized duplication of software and should be concerned about computer viruses. Therefore, only the Systems Department is authorized to download and/or install software in Court computers. Software and data on the Court's systems belong to the Court and judicial employees can not copy or remove files when they leave the Court's employment. Employees wishing to install software or hardware shall obtain the authorization from the Judicial Officer or Court Unit Executive and contact the Systems Department for installation.

Employees wishing to install their personal digital organizers (PDAs) shall obtain authorization from their judicial officers or managers before installing it. The Systems Department will only support Court owned PDAs.

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 8

Any activity that is contrary to any local or federal law or regulation, including distributing or obtaining copyrighted software or information without proper authorization from the copyright holder, is forbidden. All employees using the Court's Internet connections must respect all copyright issues regarding software, information, and authorship. With respect to software, copying copyrighted software to a Court computer without proper licensing is a copyright infringement. Any employee who has unlicensed software on Court equipment that has been provided for his or her use will be held accountable for the legal consequences. The Court expects its employees to respect the intellectual property rights of others.

Employees are responsible for protecting their own passwords. Sharing user ID's and passwords is discouraged and employees may be held accountable for misuse that occurs through such unauthorized access.

D. Proper Representation

It is the responsibility of the employees to avoid giving the impression that they are acting in an official capacity when using government office equipment for non-governmental purposes. If there is an expectation that such a personal use could be interpreted to represent the Court, then an adequate disclaimer must be used. One acceptable disclaimer is: ***"The contents of this message are mine personally and do not reflect the position of the United States District Court for the District of Puerto Rico."***

E. Privacy Expectations

The Court's computers, network system and Internet gateway are available for access by authorized users only. The Systems Department may, at any time, open, examine or monitor any file or any traffic on any computer. Anyone using the Court's systems consents to such monitoring.

F. Enforcement

1. All employees are required to sign the agreement (attached to the back of this policy) adhering to this policy. Any questions or concerns regarding this policy must be discussed with a manager or supervisor.

Policy Regarding Limited Personal Use of Government Equipment,
Including Information Technology
Page 9

2. Judicial Officers, Court Unit Executives, Managers, and Supervisors are responsible for monitoring and enforcing this policy. On an annual basis or when necessary, section managers and supervisors shall file with their Court Unit Executive a written report on the use of government office equipment, including any misuse, inappropriate or prohibited use of such equipment by employees. The Court Unit Executive or his/her designated representative may periodically inquire managers and supervisors regarding the use of government equipment by their assigned staffs.
3. The Systems Department shall develop and/or acquire suitable equipment and software to monitor use of computer systems and detect possible misuse. Such program shall monitor access to unauthorized or inappropriate sites and shall also monitor frequency of access to particular sites during regular working hours, not otherwise authorized by a Judicial Officer or Court Unit Executive. This monitoring shall be conducted in a random fashion until unlawful detection, when the monitoring may be aimed at a particular user.
4. All users will receive an orientation every year on computer security and all applicable policies.
5. Detection of a potential improper use shall be reported immediately to the Court Unit Executive. Each Court Unit Executive will take the necessary corrective action for their assigned staff. The Clerk of Court shall refer any improper use by chambers personnel to the corresponding Judicial Officer.
6. The Systems Department shall develop the monitoring program frequency as directed by the Clerk of Court.

G. Sanctions for Misuse or Inappropriate Use

Unauthorized or improper use of Court office equipment could result in loss of or limitations on use of equipment, disciplinary or adverse action (Section IX of Clerk's Office Employee Personnel Manual or applicable Court Unit personnel manual), criminal penalties and/or employees being held financially liable for improper use (18 U.S.C. § 1719). Users of the Court's computers, networks and Internet gateway are reminded that use of those systems may be monitored and are advised that if such monitoring reveals possible evidence of criminal or other improper activity, the Court may provide information regarding this activity to law enforcement officials or other government authorities.

**IT Security Policy
[2006-2]**

**Prohibition of Internet Peer-to-Peer File Sharing, Chat Rooms
And Instant Messaging**

Administrative Office of the U.S. Courts
Washington D.C.

February 2006

BACKGROUND

At its September 2005 session, the Judicial Conference of the United States adopted the computer security policies recommended by the Committee on Information Technology in its Report on Judiciary Network Security and Privacy. A copy of the Report is available on the J-Net.¹

SCOPE

This policy applies to all federal judiciary organizations, with the exception of the Supreme Court, the U.S. Sentencing Commission, and the Federal Judicial Center.

POLICY

The use of peer-to-peer file sharing, chat rooms, and instant messaging for communicating with persons or entities outside the judiciary's private data communications network is prohibited. These programs pose extraordinary security risks to the judiciary's information technology infrastructure and will, in accordance with the policy adopted by the Judicial Conference, be blocked at the Internet gateways until such time as the security risks posed by their use can be eliminated.

DISCUSSION

File sharing (using programs such as Napster, Grokster, Morpheus, and certain interactive Internet games), chat rooms, and outside instant messaging are based on Internet technologies that circumvent the security protections provided by existing network defenses. The judiciary user involved in these activities in effect opens a communications "tunnel" bypassing all security protections and invites an outside person on the Internet into the judiciary's networks, onto the court's local area network (LAN), and into the user's

¹ http://jnet/Information_Technology/Computer_Security/Policies/Network_Security_Privacy.html

computer. The outside party, having been granted access via the established tunnel connection, could then interfere with local court and network operations and expose private judiciary information to others. While there are legitimate uses for such communication tunneling tools, the limited benefit from their use is outweighed by the security risks inherent in the current technology of these tools.

Safer alternatives exist to accomplish similar communications between judiciary personnel without the accompanying security risks. For internal judiciary use, there are a number of information sharing sites on the J-Net that are currently in use and are easily and safely accessed by judiciary users for business purposes. There is an internal instant messaging system available on Lotus Notes so that judiciary users may engage in instant messaging with one another.

Since the extraordinary security risks arising from the use of peer-to-peer file sharing, chat rooms, or instant messaging with those outside the judiciary greatly outweigh the convenience of their use, these programs will be blocked at the National Internet gateways. As with any gateway blocking, if an official judiciary need should arise, the blocking can be temporarily lifted or other methods can be used to allow the needed access to a particular site. At such time as the security risks inherent in these protocols can be eliminated, the Committee on Information Technology will reconsider this policy with a view to directing that such programs not be blocked at the Internet gateways.

INFORMATION

Questions or comments concerning this policy may be directed to the IT Security Office (ITSO) at (202) 502-2350. Correspondence can be mailed to:

Robert N. Sinsheimer, Chief
IT Security Office
Office of Information Technology
Administrative Office of the U.S. Courts
One Columbus Circle, NE
Washington, DC 20544

E-mail: Robert_Sinsheimer/DCA/AO/USCOURTS

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO



Government Office Equipment Policies User Agreement

I acknowledge my responsibility to conform to the requirements set forth in the Court's Policy Regarding Limited Personal Use of Government Equipment, Including Information Technology (Revised May 4, 2006). Failure to comply may result in revocation or restriction of access to the government office equipment, as defined in the Policy Regarding Limited Personal Use of Government Equipment, Including Information Technology (Revised May 4, 2006), and, if necessary such violations will be reported to management for further review and disciplinary action. I understand the subject matter discussed in the abovementioned policy, and I agree to abide by it.

Name _____

Court Unit _____

Department _____

Supervisor _____

Employee's Signature

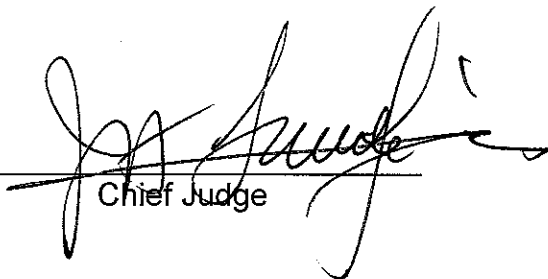
Date

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

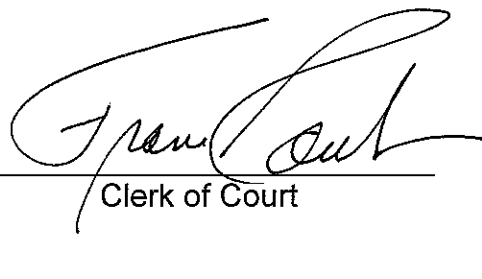


CERTIFICATION

The instant Policy Regarding Limited Use of Government Equipment, Including Information Technology was unanimously approved and adopted by the Court on August 24, 2004 and revised May 4, 2006.

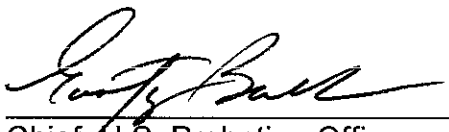


Chief Judge



Clerk of Court

Adopted



Chief, U.S. Probation Officer
Acting Chief, Pretrial Services Officer